Conjecture de Goldbach et corps de restes

Denise Chemla

Octobre 2013

1 Présentation en prose

Voici une dernière idée liée à la conjecture de Goldbach[1]: choisissons un $2p$ (p premier) qui vérifie trivialement la conjecture ($2p = p+p$). Prenons $94 = 47+47$. Dans la base de premiers $(3, 5, 7)$, $94 = (1, 4, 3)$. Les dg de 94 sont les nombres inférieurs ou égaux à 47 que trouve trc quand on lui donne les n-uplets de $\mathbb{Z}/3\mathbb{Z}\backslash\{0, 1\} \times \mathbb{Z}/5\mathbb{Z}\backslash\{0, 4\} \times \mathbb{Z}/7\mathbb{Z}\backslash\{0, 3\}$. On va essayer de trouver une bijection qui "change les restes de 94 pour passer aux restes de 88 qui est quant à lui un double de nombre composé" (en considérant chaque ensemble du produit cartésien un par un) ; cette bijection "changera les restes du dg trivial de 94 qu'est 47 pour trouver les restes d'un dg potentiel de 88". Dans la mesure où les restes d'un dg de 94, notamment ceux de son décomposant trivial 47, sont un à un différents des restes de 86 et tous non-nuls, la bijection devra être choisie de manière à préserver l'inégalité des restes du dg de 88 aux restes de 88 ainsi que préserver leur non-nullité. Peut-être qu'il y aura tellement de possibilités combinatoires de trouver une telle bijection préservant simplement l'inégalité et la non-nullité que cela assurera l'existence d'un dg pour le double de composé également, dans l'intervalle $[3, n/2]$.

On comprend que si p_k et p_{k+1} sont deux nombres premiers successifs (par exemple 5 et 7), et qu'on recherche les dg des nombres pairs compris entre $p_k^2 + 1$ à $p_{k+1}^2 - 1$ (en l'occurrence entre 50 et 120), on a seulement à considérer les restes modulaires des nombres selon les nombres premiers appartenant à $Prem(n) = \{3, 5, 7\}$ (on peut appeler cet ensemble la base du codage).

2 Outils

Le nombre de bijections d'un ensemble de cardinal n dans lui-même est $n!$.

Dans un premier temps, nous souhaitions établir le "passage de la décomposition triviale d'un double de premier à une décomposition de Goldbach d'un double de composé" concerné par une même base, i.e. qui est compris entre deux carrés de premiers consécutifs. Malheureusement, rien n'assure encore l'existence d'un double de premier entre deux tels carrés.

On s'est donc rabattu (et cela nécessitera peut-être simplement de mener un raisonnement par récurrence) sur l'idée qui consiste à établir le "passage de la

[1] Tout nombre pair supérieur ou égal à 4 est la somme de deux nombres premiers.

décomposition triviale d'un double de premier $2p_k$ vers une décomposition de Goldbach d'un pair double de composé" pour tout double de composé inférieur à $2p_k$ et supérieur à $2p_{k-1}$ (en fait, c'est ici que j'ai un gros problème : si je garde la base, les nombres obtenus par trc peuvent être trop grands, ils peuvent aller jusqu'au produit des modules (auquel on soustrait 1). Si du coup, je décide d'effectuer le passage seulement vers des pairs "assez petits pour être tranquille", par exemple les pairs compris entre $p_i^2 + 1$ et $p_{i+1}^2 - 1$ avec $p_{i+1}^2 - 1 < 2p_k$, je crains qu'ils soient alors si petits qu'à nouveau, la solution minimale du trc qui peut aller jusqu'au produit des modules ne dépasse leur moitié.).

3 Inventer une bijection

On aimerait établir les correspondances suivantes, où p_1 et p_2 sont des nombres premiers tandis que c est un nombre composé (g est la fonction qui associe à un nombre l'un de ses dg, on note g_t la fonction qui associe au pair double d'un nombre premier son dg trivial) :

$$\begin{array}{ccc} 2p_1 & \xrightarrow{f} & 2c \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ p_1 & \xrightarrow{f} & p_2 \end{array}$$

Par exemple, pour $94 = 2.47$ et $88 = 2.44$, on aurait :

$$\begin{array}{ccc} 94 = (1,4,3) & \xrightarrow{f} & 88 = (1,3,4) \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ 47 = (2,2,5) & \xrightarrow{f} & 29 = (2,4,1) \end{array}$$

Les bijections à l'œuvre dans l'exemple ci-dessus seraient :

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ \mathbb{Z}/3\mathbb{Z}\backslash\{0,1\} \times \mathbb{Z}/5\mathbb{Z}\backslash\{0,4\} \times \mathbb{Z}/7\mathbb{Z}\backslash\{0,3\} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z}\backslash\{0,1\} \times \mathbb{Z}/5\mathbb{Z}\backslash\{0,3\} \times \mathbb{Z}/7\mathbb{Z}\backslash\{0,4\} \end{array}$$

Pour f, on peut prendre la fonction $f_1 \times f_2 \times f_3$ avec f_1, la permutation de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$ Id, f_2, la permutation de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/5\mathbb{Z}$ $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 3 \end{pmatrix}$ et f_3, la permutation de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/7\mathbb{Z}$ $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$.